REMARKS

This Amendment is in response to the Office Action mailed November 8, 2005.

In the Office Action claims 9-14 and 15-19 are rejected under 35 U.S.C. §102(e) as being anticipated by Brown et al. (US 2004/0139327 A1). Claims 20 and 24-28 are rejected under 35 U.S.C. 102(e) as being anticipated by Ginter et al. (US 2005/0060584). Claims 1-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Brown et al. in view of Ramanathan (US 2002/0144110 A1) and further in view of Aucsmith et al. (US 5,712,914). Claims 21-23 are rejected under 35 U.S.C. §103(a) as being unpatentable over Ginter et al. in view of Brown et al.

The present amendment amends independent claim 1 to incorporate the subject matter of dependent claim 6. Claim 6 is canceled. Independent claim 9 has been amended to incorporate the subject matter of dependent claim 14. Claim 14 has been canceled. Independent claim 15 is maintained as originally filed. Independent claim 20 has been amended to incorporate the subject matter of dependent claims 25 and 26. Dependent claims 25 and 26 have been canceled. Lastly, new independent claim 29 is presented herewith. New independent claim 29 incorporates the subject matter of originally filed independent claim 1 and that of originally filed dependent claim 7. New dependent claims 30-33 are presented herewith and depend upon new independent claim 29.

Amended independent claim 1 and its dependent claims

As amended, claim 1 recites:

> **... the authority of the user defined within the second code portion of the certificate being verifiable by the server computer independently of the digital certificate by accessing a store of authority information that is independent of the digital certificate.**

In support of the rejection of the subject matter of claim 6 (corresponding to the added underlined recitations in amended claim 1), the Examiner points to paragraphs [0165], [0174] and [0183] of Brown et al., as well as to selected passages of Ramanathan and Aucsmith et al.

Paragraph [0165] of Brown et al. teaches the certificates are stored in a publicly accessible repository and are accessed using LDAP. Such an LDAP repository of digital certificates does not meet the requirements of amended claim 1 so that the authority of the user is independent of the digital certificate. Moreover, paragraphs [0174] and [0183] only disclose checking the digital certificate for the certificate holder's maximum signing authority (e.g., $1000.00 in the example given). Neither this paragraph nor the remainder of Brown et al. teaches that the authority of the user is verifiable by accessing a store of authority that is independent of the digital certificate, as claimed. In fact, [0184] and [0185] of Brown et al. teaches that if the amount of the payment request does not exceed the signer's maximum payment authority, "the method continues by completing 892 the electronic transaction." There is no teaching or suggestion in Brown et al. that the authority defined in the digital certificate is verifiable by accessing a store of authority that is independent of the digital certificate – quite to the contrary. The Ramanathan and Aucsmith et al. references do not remedy the shortcomings of the primary reference to Brown et al., even when considered in combination with Brown et al. Indeed, the teachings of Ramanathan regarding the structure of the digital certificate relative to the claimed first and second code portions and the extension field of Aucsmith et al.'s digital certificate, even when combined with Brown et al., does not teach or suggest that the authority of the user defined in the second code portion is verifiable by accessing a store of authority that is independent of the digital certificate, as required by amended independent claim 1.

Reconsideration and withdrawal of the §102(e) rejection applied to independent claim 1 and its dependent claims are, therefore, respectfully requested.

Amended independent claim 9 and its dependent claims

As amended, independent claim 9 recites:

> **... validating the authority information included within the received certificate by accessing a store of authority information that is independent of the received certificate, and**
>
> **executing of the payment request only when the certificate-identifying information, the user-identifying information and the authority information within the received certificate is successfully validated.**

In support of the rejection of the subject matter of claim 14 (corresponding to the added underlined recitations in amended claim 9), the Examiner points to Figs. 1-3, 8, paragraphs [0165], [0174], [0183], and claim 80 of Brown et al.

At the outset, paragraph [0165] teaches that the certificates are stored in a publicly accessible repository that may be accessed using a protocol such as LDAP. Paragraph [1074] clearly states that Brown et al. checks a document for an electronic payment request and authorizes payment based upon the authority of the signer. No validation is taught here, much less any validation in which the authority information within the received certificate is validated by accessing a store of authority information that is independent of the received certificate. The LDAP accessible repository of [0165] cannot be the claimed independent store, as it is a repository of the certificates themselves – which cannot, by definition, be independent of the received certificate, as required by amended claim 9. Paragraphs [0183], [0184] and [0185] of Brown et al. teach that if the amount of the payment request does not exceed the signer's maximum payment authority, "the method continues by completing 892 the electronic transaction." There is no teaching or suggestion in Brown et al. that the authority defined in the digital certificate is verifiable by

accessing a store of authority that is independent of the digital certificate, again as required by amended claim 9. Claim 80 of Brown et al. is even more explicit:

> **The system claim 21, wherein the processing instruction is a payment processing instruction, the payment processing instruction identifying within the document at least one electronic payment request to process, the electronic payment request including an indication of a payment amount, the electronic payment request being digitally signed by a signer's digital signature; the at least one processing service comprising: a payment processing service adapted to identify the electronic payment request from the payment processing instruction, obtain a digital certificate indicating a maximum signing authority for the signer and complete the electronic payment request when the payment amount does not exceed the signer's maximum signing authority. (Underlining added for emphasis)**

Therefore, Brown et al. teach that to complete the electronic payment request as long as the payment amount does not exceed the signer's maximum signing authority. No independent validation of any authority information is carried out or taught in Brown et al.

It is, therefore, respectfully requested that the 35 USC §102(e) rejection applied to independent claim 9 and its dependent claims be withdrawn and not re-applied to amended independent claim 9 and its dependent claims.

Independent claim 15 and its dependent claims

Originally filed independent claim 15 recites:

> **... authorization validating code configured to enable validation of the authority information within the received certificate against corresponding authority information for the user stored in a data structure that is independent of the received certificate.**

Therefore, the same validation step is carried out in independent claim 15 as is claimed in independent claim 9 and as discussed immediately above. Independent claim 15 is rejected on exactly the same basis and enumerated figures, paragraphs and claims of Brown et al. as is independent claim 9. It is not believed necessary to repeat these arguments here. Instead, Applicant's representative expressly incorporates such arguments here as if repeated in full.

Independent claim 20 and its dependent claims

As amended, independent claim 20 recites:

> **... allowing each selected secondary employee to exercise only those rights within the computing environment that are granted by the secondary rights defined within the assigned secondary certificate, and**
>
> **revoking a secondary certificate to a terminated secondary employee, the revoking step being operative to revoke all certificates to secondary employees of the company that report to the terminated secondary employee, and to revoke all secondary rights that are derivative from the secondary rights granted by the revoked secondary certificate.**

In support of the rejection of the subject matter of claim 25 and 26 (corresponding to the added underlined recitations in amended claim 20), the Examiner points to claim 59 of Ginter et al. However, claim 59 of Ginter et al. merely recites that the electronic archive (that stores keys and digital certificates according to Ginter et al.'s claim 57) further stores a list of revoked digital certificates. The only other teachings of revoked certificates is found in paragraph [0901] of Ginter et al., reproduced below for the Examiner's convenience:

> **[0901] Certifying authority 500 may also maintain a revocation list 542 based on trustedness data 540 indicating, for example, certificates that have been compromised or that previously certified facts are no longer true (for example, Mr. Smith used to be a Stanford University professor but has since left the University's employ). The maintained revocation list function 526 is important for providing a mechanism to ensure that "bad" certificates cannot continue to be used once they are known to be bad. Certificates 504 issued by certifying authority 500 can expire, and the certifying authority can (for example, for a fee) renew a previously issued certificate by performing certificate renewal function 532. The certifying authority 500 may maintain a record or database of the certificates it has issued, and this database can be distributed--which can benefit from replication function 536 and propagation function 538 to accurately and efficiently distribute the database across a number of different locations.**

As the Examiner can see, there is no teaching in Ginter et al. of any step of revoking a secondary certificate to a terminated secondary employee, in which the revoking step is operative to revoke all certificates to secondary employees of the company that report to the terminated secondary employee, and to revoke all secondary rights that are derivative from the secondary

rights granted by the revoked secondary certificate, as claimed and required by amended claim 20. Failing such, it is respectfully submitted that amended claim 20 must be allowed.

New independent claim 29 and its dependent claims

New independent claim 29 incorporates the subject matter of originally filed independent claim 1 and that of originally filed dependent claim 7. The outstanding Office Action rejected dependent claim 7 as being unpatentable over a combination of Brown et al., Ramanathan and Aucsmith et al., but points specifically to paragraph [0183] of Brown et al. as teaching the subject matter of claim 7.

New independent claim 29 recites:

> **... the authority of the user defined within the second code portion of the certificate defining access rights of the user to data and programs within the computing environment.**

It is to be noted that Brown et al.'s disclosure of authority is limited to a specific dollar amount as the signing authority. Indeed, paragraph [1083] states:

> **[0183] If, however, the signature was successfully verified, the method continues by checking 886 the digital certificate corresponding to the signature 118 for the maximum signing authority of the signer. Under X.509 version 3, the digital certificate may specify a maximum signing authority. For example, a signer may only be authorized to digitally sign payment requests up to $1000.00. Thus, the digital certificate of the signer will indicate a maximum signing authority of $1000.00.**

There is no teaching therein of the authority defining any access rights of the user to data and programs within a programming environment, as recited by new independent claim 29.

Brown et al.'s claim 39 is also representative of the authority (only $ amounts) disclosed in this reference:

> **49. The method of claim 21, wherein the processing instruction is a payment processing instruction, the payment processing instruction identifying within the document at least one electronic payment request to process, the execution step comprising: identifying the electronic payment request to**

> **process from the payment processing instruction, the electronic payment request including an indication of a payment amount, the electronic payment request being digitally signed by a signer's digital signature; obtaining a digital certificate corresponding to the signer's digital signature, the digital certificate indicating a maximum signing authority for the signer; checking the digital certificate for the signer's maximum signing authority; and completing the electronic payment request when the payment amount does not exceed the signer's maximum signing authority.**

Indeed, Brown et al. teach the "maximum signing authority" of a certificate holder, by which Brown et al. invariably mean a specific dollar amount, and not access rights to data and/or programs, as claimed in new independent claim 29. Applicant's representative is mindful of the requirement to consider §103(a) references in combination. Therefore, the references to Brown et al., Ramanathan and Aucsmith et al. must be evaluated collectively for what they teach and/or suggest to one of ordinary skill in the art. However, Ramanathan is relied upon for his teaching of first and second code portions, whereas Aucsmith et al. is relied upon for its teaching of a digital certificate with an extension field. Therefore, Ramanathan and Aucsmith et al. do not remedy the fundamental shortcomings of Brown et al. relative to new independent claim 29, in that Brown et al. do not teach, whether considered singly or in combination with the two secondary references, that "the authority of the user defined within the second code portion of the certificate defining access rights of the user to data and programs within the computing environment" as claimed herein.

In view of the foregoing, it is respectfully submitted that new independent claim 29 is allowable over the applied art.

Applicant believes that this application is now in condition for allowance. If any unresolved issues remain, please contact the undersigned attorney of record at the telephone number indicated below and whatever is necessary to resolve such issues will be done at once.

Respectfully submitted,

Date: Jan 11, 2006 By: _____

Alan W. Young
Attorney for Applicant
Registration No. 37,970

Young Law Firm, P.C.
4370 Alpine Rd., Ste. 106
Portola Valley, CA 94028
Tel.: (650) 851-7210
Fax: (650) 851-7232

\\Ylfserver\ylf\CLIENTS\ORCL\5881 (OID-2003-142-01)\5881 AMEND.1.doc